



# Desarrollo seguro en Python

## Lección 2: OWASP TOP 10

# Identificado vulnerabilidades

**A continuación, se describe un ataque a una aplicación del sistema de salud de la seguridad social. Debes identificar el número de vulnerabilidades del OWAS TOP 10 y justificar las que identifiques.**

## Objetivos

- | Identificar OWASP TOP 10 sobre un ataque a una aplicación.

## Contenido correspondiente a lección 2: OWASP TOP 10

### Actividad relacionada con la lección 2:

#### Descripción de lo sucedido.

Tenemos una aplicación web que recoge el parámetro id y lo asigna automáticamente a una consulta SQL.

```
String query = "SELECT * FROM datosmedicospacientes WHERE custID='" +  
request.getParameter("id") + "'";
```

El resultado de la consulta se mostraría en el navegador web. El atacante ha conseguido pasar el siguiente parámetro sobre id mediante la aplicación SQLmap.

```
http://saludseguridadsocial.com/app/accountView?id=' or '1'='1
```

Ha conseguido acceder a varios expedientes médicos y nuestro sistema no nos ha informado del ataque. Nos hemos enterado porque el atacante nos ha enviado un email con los expedientes.